IN THE CLAIMS

For the Examiner's convenience, all pending claims are included below.

1. (Original) A method comprising:

requesting a desired service through a foreign service provider;

generating a hash tree and generating a digital signature on a root value of the hash tree;

sending the digital signature and the root value to the foreign service provider;

providing one or more tokens to the foreign service provider with the next packet if the foreign service provider accepts the signature; and

continuing to use the service while the foreign service provider accepts tokens.

2. (Original) The method of Claim 1 further comprising a user device generating the one or more tokens.

3. (Original) The method of Claim 2 wherein the user device generates tokens using the hash tree.

4. (Original) The method of Claim 3 wherein the hash tree comprising a dense hash tree, and further comprising constructing the dense hash tree by:

randomly generating a number of bit streams equal to the number of tokens that is estimated to be needed;

constructing a binary tree with a number of leaves equal to the number of estimated tokens plus one;

assigning the random bit strings to the leaves; and

computing values to be assigned to each internal node according to the values of children of internal nodes.

5. (Original) The method defined in Claim 4 wherein generating a number of bit streams comprises generating the number of bits streams from a single seed.

6. (Original) The method of Claim 4 wherein the bit strings are of cryptographically suitable length.

7. (Original) The method of Claim 3 wherein the hash tree is one selected from a group consisting of a Merkle tree and a dense hash tree.

8. (Original) The method of Claim 1 wherein the user device generates the one or more tokens using a public key signature scheme, including using a public-key signature to sign the root of the hash tree.

9. (Original) The method of Claim 1 further comprising generating a digital signature on the root of the tree using a private signing key.

10. (Original) The method of Claim 1 wherein the user device includes in each of the one or more of the tokens one or more of a group consisting of the identity of the foreign service provider for which tokens are intended, a maximum number of tokens that the foreign service provider may receive, and any conditions that the foreign service provider must satisfy before it can redeem the token.

11. (Original) The method of Claim 1 further comprising sending to the foreign service provider a signature on the root value of the hash tree, a public key of the user device and a certificate from a trusted party attesting to a relationship between the user and their service provider.

12. (Original) The method of Claim 1 wherein the token is an undeniable token.

13. (Original) The method of Claim 1 comprising:

generating a dense hash tree;

providing the root value to a home service provider for signature;

informing the home service provider of the monetary value of the dense hash tree; and

providing payments based on the tree to the foreign service provider.

14. (Original) An apparatus comprising:

an external network interface through which a request for a desired service of a foreign service provider is made;

a memory;

a processor coupled to the external network interface and the memory, wherein the processor generates a hash tree and generates a digital signature on a root value of the hash tree using the memory, and further wherein the processor sends the digital signature and the root value to the foreign service provider, via the external network interface, along with one or more tokens with the next packet if the foreign service provider accepts the signature, and continues to use the service while the foreign service provider accepts tokens.

15. (Original) The apparatus of Claim 14 further comprising a user device generating the one or more tokens.

16. (Original) The apparatus of Claim 15 wherein the user device generates tokens using the hash tree.

17. (Original) The apparatus of Claim 16 wherein the hash tree is one selected from a group consisting of a Merkle tree and a dense hash tree.

18. (Original) The apparatus of Claim 14 wherein the processor generates the one or more tokens using a public key signature scheme, including using a public-key signature to sign the root of the hash tree.

19. (Original) The apparatus of Claim 14 wherein the processor includes in each of the one or more of the tokens one or more of a group consisting of the identity of the foreign service provider for which tokens are intended, a maximum number of tokens that the foreign service provider may receive, and any conditions that the foreign service provider must satisfy before it can redeem the token.

20. (Original) The apparatus of Claim 14 wherein the processor causes a signature on the root value of the hash tree, a public key of the user device and a certificate from a trusted party attesting to a relationship between the user and their service provider to the foreign service provider via the external network interface.

21. (Original) The apparatus of Claim 14 wherein the token is an undeniable token.

22. (Original) The apparatus of Claim 14 wherein the processor provides a root value of a dense hash tree to a home service provider for signature and informs the home service provider of the monetary value of the dense hash tree to enable the home service provider to pay the foreign service provider for the service.

23. (Original) An apparatus comprising:

means for requesting a desired service through a foreign service provider;

means for generating a hash tree and generating a digital signature on a root value of the hash tree;

means for sending the digital signature and the root value to the foreign service provider;

means for providing one or more tokens to the foreign service provider with the next packet if the foreign service provider accepts the signature; and

means for continuing to use the service while the foreign service provider accepts tokens.

24. (Original) An article of manufacture having one or more recordable media storing instructions thereon which, when executed by a system, cause the system to perform a method comprising:

requesting a desired service through a foreign service provider;

generating a hash tree and generating a digital signature on a root value of the hash tree;

sending the digital signature and the root value to the foreign service provider;

providing one or more tokens to the foreign service provider with the next packet if the foreign service provider accepts the signature; and

continuing to use the service while the foreign service provider accepts tokens.

25.-54. (Cancelled)